A Groundhog Day in Brussels

Genna Chuches 2020-07-16T16:37:05

16 July 2020 feels like Groundhog Day in Brussels. For those, who did not see the famous film Groundhog Day, it's about reliving the same experience again and again until the main protagonist gets 'why'. Similarly, the much anticipated *Schrems II* decision, delivered by the Court of Justice of the European Union (CJEU) today, is almost a 'reliving' of its earlier decision in *Schrems I*: today the CJEU invalidated the (in)famous Privacy Shield Decision ('Privacy Shield'), succeeded its predecessor Safe Harbour Decision ('Safe Harbour'), which the same Court declared invalid back in 2015 in *Schrems I*. The Court also upheld the validity of the SCC Decision and the use of standard contractual clauses for international data transfers, ruling that National Data Protection Authorities ('DPAs') *must* act where these clauses do not provide safeguards equivalent to the *General Data Protection Regulation* ('*GDPR*'). *Schrems II* thus is the latest chapter in the continued ideological battle initiated by the 'CJEU' against the ever-expanding US tech surveillance infrastructure — a tussle which shows no signs of abating. How many 'Schrems' are we going to have — and who is the protagonist that needs to get 'why'? Let's look at it all in more detail.

Background

Schrems II is the second decision stemming from the long running challenge of Facebook Ireland's transfers of personal data to the US by data protection and privacy activist Maximillian Schrems. Following the Snowden revelations about US mass surveillance programmes in 2013, Schrems lodged a complaint with the Irish Data Protection Commissioner ('DPC') about Facebook Ireland's transfer of data to the US under the Safe Harbour Decision ('Safe Harbour'), as US surveillance meant his data was not afforded EU equivalent protections. Safe Harbour was a European Commission decision declaring the adequacy of protections under an EU-US arrangement where US data importers could 'self-certify' that they provided EU equivalent data protection. In 2013, the Irish DPC rejected Schrems' complaint, which he subsequently took to the High Court of Ireland, which referred two questions to the Court of Justice of the European Union ('CJEU'). In that reference for preliminary ruling — now widely known as *Schrems I* — *Schrems v Data Protection Commissioner* the CJEU invalidated Safe Harbour which had authorised personal data transfers from the EU to US since 2000 (*Schrems I* [98], [104]-[106]), finding transfers made under Safe Harbour were not afforded essentially equivalent protection to that guaranteed under EU law. The CJEU returned Schrems' complaint to the DPC after determining, in line with *Commission v Hungary* [53] that DPAs are the 'guardians' of fundamental rights, and *must* be able to examine claims concerning the protection of rights and freedoms for data transferred to a third country.

In 2016, shortly after *Shrems I*, Safe Harbour was replaced with Privacy Shield which established another US 'self-certified' regime for EU-US data transfers, albeit

within a more restricted framework than Safe Harbour. The DPC re-opened its investigation, requesting Mr Schrems to reformulate his original complaint in light of the invalidation of Safe Harbour. That reformulation challenged Facebook's data transfers outside of the EU based on SCC's. Privacy Shield was not in place at the time Schrems reformulated complaint was lodged (*Schrems II* [151,-[153]). SCC are contractual clauses, agreed between the data exporter (i.e. Facebook Ireland) and data importer, (i.e. Facebook US) used by data controllers to assure essentially equivalent data protection in a third country. Schrems' claimed the reliance on SCCs could not be valid due to US local obligations to provide access to personal data to public authorities under US surveillance programs, thus failing to ensure adequate protection for data transferred outside the EU.

Based on Schrems' new complaint, the DPC raised a number of questions before the High Court of Ireland, which subsequently referred 11 questions to the CJEU in *Schrems II*. These questions turned the focus towards the suitability and validity of SCCs and by inference, the validity of Privacy Shield. *Schrems II* presented the CJEU with another opportunity to articulate data protection requirements for international data transfers, in what has turned out to be Groundhog Day for EU-US adequacy decisions.

CJEU Decision

The CJEU first held that although the complaint was brought under the *EU Data Protection Directive*, which has since been repealed, the questions would be answered under the *GDPR* [79]. The Court affirmed that the *GDPR* applies to the transfer of data to a third country for processing for a commercial purpose [86], irrespective of further processing by public authorities for national security purposes [89]. Determining that SCCs can be validly used [105], the CJEU outlined that an assessment of the level of protection afforded under SCCs should include the agreed contractual clauses between the data controller and the third country recipient/processor, any access by public authorities to the data and the legal system of the third country [105] with the thresholds required outlined under Chapter V of the *GDPR* [93]. The responsibility to suspend, limit, or even ban international data transfers where they do not provide the 'essential equivalent' of EU law, was again thrust upon DPAs, particularly where they formed the view that SCCs are not or cannot be complied with in the third country [113], [121]. This obligation to act is tempered only by the presence of an adequacy decision such as Privacy Shield, validating transfers to the third country. In those circumstances, the Court explained, the DPA must be able to investigate a complaint, and where the investigation reveals doubts about the safeguards provided, they should bring the matter before then national courts who may then refer the matter for a preliminary ruling on the validity of the adequacy decision [120], [157]. Data controllers still have an obligation to act first: where they are exporting data and there is a conflict between the SCC and local laws, the data controller should suspend data flows [134]-[135]. In situations where Member States' DPAs adopt diverging decisions about the adequacy of safeguards in third countries, the CJEU highlighted that the matter should be referred to the European Data Protection Board for an opinion [147]. SCCs were found to be a valid

mechanism for ensuring essentially equivalent protections in third countries and as such the SCC Decision was found to be valid [148]-[149].

In a departure from the A-G Opinion, the Court chose to engage with the validity of Privacy Shield and declared it invalid [199]. In essence, this is because of the Court's findings that DPAs cannot act against an adequacy decision, such as Privacy Shield, without raising the validity of the decision with their national courts, who may, if they agree with the DPA, request a preliminary ruling by the CJEU. In other words, the Irish DPC would have been prohibited from stopping, limiting or prohibiting data flows based on Schrems' complaint if Privacy Shield remained valid. On this matter the Court specifically said 'Privacy Shield decision is binding on the supervisory authorities insofar as it finds that the United States ensures an adequate level of protection' [156].

The Court engaged in an assessment of the adequacy assured by the United States [178]-[198]. In short, the Court affirmed concerns over US surveillance laws including section 702 of the FISA and Executive Order 12333 [178], ultimately finding that neither, when read in conjunction with Presidential Policy Directive PPD-28 'correlates to the minimum safeguards resulting, under EU law, the principle of proportionality, with the consequence that the surveillance programs based on those provisions cannot be regarded as limited to what is strictly necessary' [184]. The Privacy Shield decision determined that the US provides essentially equivalent safeguards, yet, the Court found US surveillance laws were not sufficiently circumscribed to meet that threshold[185]. Further, the Court assessed the right to redress under the ombudsperson regime was deficient with at least some mechanisms of surveillance not covered [191], [192]. Finally, it was criticized that the ombudsperson was not independent from the executive [195]. The Court concluded that for these reasons the Privacy Shield decision was invalid due to incompatibility with Article 45(1) of the *GDPR* [199].

Was the Invalidation of Privacy Shield Expected?

Schrems II was the second EU-US decision on adequacy invalidated in a period shorter than five years. With over 5000 companies certified under Privacy Shield, similar numbers to those certified under Safe Harbour, the invalidation of Privacy Shield will have significant implications for data transfers to the US.

With findings of the Irish High Court that the US carries out mass and indiscriminate data processing risking violation of Arts 7 and 8 of the Charter [193], the invalidation of Privacy Shield was not unexpected. Comments in the *Schrems II* AG Opinion on Privacy Shield's validity [340], [341] supported the overall CJEU finding that data transfers can only be made where the third country provides essentially equivalent EU law protection. The invalidation again questions the ability of a 'self-certified' agreement, such as Privacy Shield, to maintain EU levels of protection where local laws have an extensive surveillance focus.

The political climate in the EU surrounding Privacy Shield was also negative. The European Parliament's Civil Liberties Committee has repeatedly recommended that

the Privacy Shield was inadequate and the EP has called on the EU Commission to review the scheme . The 2017 amendments to the US *Foreign and Intelligence Surveillance Act*, extending the controversial surveillance scheme raised concerns at the European Parliament , and the failure to roll out the *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services Act* in 2017, fuelled the criticism of the federal US data protection regime. The Cambridge Analytica scandal has further highlighted that if Privacy Shield was to be maintained, it required better monitoring. Finally, the highly contentious 2017 *CLOUD Act* which permit US access to data held by US companies across the globe, have also raised concerns at the EP. The interplay between EU data protection law, its potential effects on Privacy Shield and its ability to circumvent existing MLAT (Mutual Legal Assistance Treaty) processes have been questioned. The exact interaction between the *CLOUD Act*, Privacy Shield and EU data protection law is unclear.

Implications for SCCs

Schrems II will have significant implications for data transfers to third countries, including the post-Brexit UK, because SCCs are relied on by 88 per cent of EU companies transferring data outside the EU. With data controllers being the first layer of protection under the SCC regime, and specific requirements outlined for these agreements, including a finding of inadequacy of US laws, it is anticipated that the next several months will be consumed by data exporters/controllers re-evaluating current SCCs. In light of the Court's ruling that DPA's must act on user complaints where data transfers under SCCs do not afford equivalent EU law protections, the pressure will be on data controllers to ensure compliance.

Of course, if SCCs are to be effective mechanisms of EU law, DPAs must be prepared to use their *Schrems II*-mandated powers confidently, adopting corrective measures where data controllers fail to act or make agreements under SCCs which do not afford protection which is an essential equivalent of EU law.

Conclusion

Following the Snowden revelations in 2013, the CJEU has been very vocal on the constitutional significance of data protection in EU legal framework well beyond the Schrems' saga. *Digital Rights Ireland v Minister for Communications*, *Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson*, *Opinion 1/15 (Passenger Name Records)* and *Constantin Film Verleih v YouTube LLC and Google* have demonstrated the CJEU's persistence in ensuring EU fundamental rights are protected in a world where surveillance is becoming the norm, not the exception.

Schrems II has reinforced the fundamental role of data protection in the EU legal order and transatlantic relations, demonstrating that it will not accept 'second rate' protection for personal data transferred outside EU. It has also reasserted the DPA's power to suspend, limit, or even ban data transfers to countries where EU fundamental rights are not protected. It remains to be seen if DPA's, in their newly

affirmed role as the gatekeepers of international data transfers, will wield their powers and close the gates to data flows where they fall below the standards of the EU law. One thing is certain, the CJEU's fight to ensure the role for data protection in international data flows is not yet over. And we may see another Groundhog Day.
